REMARKS

The present Amendment amends claims 5-10 and 19-24, leaves claims 11, 13, 15 and 17 unchanged and cancels claims 14 and 18. Therefore, the present application has pending claims 5-11, 13, 15, 17 and 19-24.

The drawings stand objected to under 37 CFR §1.83(a) being that the Examiner alleges that the drawings must show every feature of the invention specified in the claims. Particularly, the Examiner alleges that the drawings do not illustrate the limitation of "a plurality of clients" as recited in the claims. This objection is traversed for the following reasons. Applicants submit that the drawings do in fact illustrate the limitation of "a plurality of clients" as recited in the claims.

The Examiner's attention is directed to Fig. 4 in which the client content distribution permission database 450 is illustrated as having at least two clients, namely client 1 and client 2. A discussion of these features of the present invention can be found in the present application in the last paragraph on page 6 and the last paragraph on page 12.

Thus, the drawings do illustrate the limitation of "a plurality of clients" as recited in the claims. Therefore, reconsideration and withdrawal of this objection is respectfully requested.

Claims 5-7, 10, 11 and 15 stand rejected under 35 USC §102(e) as being anticipated Datta (U.S. Patent No. 6,622,168); claims 8, 9, 14 and 18 stand rejected under 35 USC §103(a) as being unpatentable over Datta in view of Alegre (U.S. Patent No. 6,199,113); claims 13 and 17 stand rejected under 35 USC §103(a) as being unpatentable over Datta in view of Scott (U.S. Patent No. 6,338,094); claims 19, 21 and 23 stand rejected under 35

USC §103(a) as being unpatentable over Datta in view of Alegre and further in view of Horvitz (U.S. Patent No. 6,182,133); and claims 20, 22 and 24 stand rejected under 35 USC §103(a) as being unpatentable over Datta in view of Alegre and further in view of Li (U.S. Patent Application Publication No. 2004/0210604). As indicated above, claims 14 and 18 were canceled. Therefore, the above described rejection of claims 14 and 18 under 35 USC §103(a) as being unpatentable over Datta in view of Alegre is rendered moot. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

With respect to the remaining claims, the above described rejections of said claims are traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 5-11, 13, 15, 17 and 19-24 are not taught or suggested by Datta, Alegre, Scott, Horvitz or Li whether taken individually or in combination with each other as suggested by the Examiner. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw these rejections.

Amendments were made to each of the independent claims so as to more clearly describe features of the present invention. Particularly, amendments were made to each of said independent claims to more clearly describe, for example, features of the present invention as illustrated in steps 202, 203, 205, 125, 127, 128 and 129 of Fig. 2 and steps 523 and 524 of Figs. 5 and 6. These amendments made to the claims now more clearly recite that once contents expected to be in demand in the future have been collected from the content server, a client which requests contents from the collected contents must first obtain permission to access the collected contents. These

amendments made to the claims further recite that once the client has obtained permission to access the collected contents, requested contents are distributed in an encrypted form and the encrypted form is distributed along with a decryption key so as to allow the client having permission to decrypt the encrypted requested content using the decryption key upon receipt thereof in the client.

The above described features of the present invention now more clearly recited in the claims provides enhanced security so that at a first layer of security only clients that have permission can access the collected content and then at a second layer of security distributed requested contents are encrypted and distributed along with a decryption key so that only the client having permission and having the decryption key can decrypt the encrypted content.

The above described features of the present invention now more clearly recited in the claims are not taught or suggested by any of the references of record whether taken individually or in combination with each other. Particularly the above described features of the present invention now more clearly recited in the claims are not taught or suggested by Datta, Alegre, Scott, Horvitz or Li whether said references are taken individually or in combination with each other as suggested by the Examiner.

Numerous arguments were presented distinguishing the features of the present invention from the references of record were presented in the Remarks of the March 16, 2006 Amendment. The Remarks of the March 16, 2006 Amendment are incorporated herein by reference.

In the Office Action the Examiner readily admits that Datta does not teach or suggest apparatus for distinguishing a client so that only clients having permission to access the contents are allowed to access the content as in the present invention. Further, the Examiner readily admits that Datta does not teach or suggest that the contents upon distribution to a client is encrypted and a decryption key is supplied to the client so as to permit decryption of the encrypted content upon its receipt in the client as in the present invention.

The Examiner recognizing these deficiencies of Datta, attempts to supply these deficiencies by combining the teachings of Datta with Alegre.

In the Office Action the Examiner alleges that Alegre teaches apparatus for distinguishing clients so as to allow only clients having permission to access the database and teaches the use of a decryption key to decrypt encrypted content when distributed to the clients.

It seems that the Examiner has completely mis-described the teachings of Alegre in an attempt to meet the features of the present invention as recited in the claims. At no point is there any teaching or suggestion in Datta or Alegre of the above described features of the present invention now more clearly recited in each of the independent claims.

For example, Alegre does teach the use of an authentication server 226 which authenticates a client by allowing the client 110 to input a user ID and a password which are compared to pre-stored authentication information. In Alegre the authentication server 226 upon detecting that the user ID and the password corresponds to a user allowed to access the content then creates a "unique and un-predictable session key" which is transmitted to the

client 110. The session key as taught by Alegre is not used for encryption or decryption purposes. The session key is simply used as a mechanism to uniquely identify and authenticated client.

As taught by Alegre the client 110 sends a request for a particular URL to the web host 210 along with the session key. The web host 210 as taught by Alegre processes the request and the session key to create a network request packet which is transmitted to the access server 222. As per Alegre, the access server 222 verifies that the network request packet came from the web host 210, extracts the session key from the network request packet and then verifies whether the session key is valid. If the session key is valid, the access server 222 performs the requested operation including obtaining requested information according to the network request packet from the database 134.

Thus, in Alegre the session key which is supplied to the client 110 simply allows the client 110 to obtain permission to access the database 134. Attention is directed to the teachings of Alegre in col. 4, line 24 through col. 5, line 6. No encryption or decryption is involved with the session key as taught by Alegre.

Alegre further teaches that all accesses to the database 134 by the client 110 via the trusted network 138 are handled by communications between the web host 210 and the access server 222. Alegre teaches, for example, that the web server 210 includes a speaker object 514 as illustrated in Fig. 5 that communicates with a listener object 1212 of the access server 222 as illustrated in Fig. 12.

Alegre specifically teaches that only the network request packet sent from the speaker object 514 of the web host 210 to the listener object 1212 of the access server 222 can be encrypted. There is absolutely no teaching or suggestion in Alegre that the content returned to the client 110 in response to the network request packet from the client 110 is encrypted and distributed to the client 110 along with a decryption key to allow for the encrypted content to be decrypted at the client 110 as in the present invention as recited in the claims.

Alegre specifically teaches, for example, in col. 7, lines 27-37 that:

> "The packet created by speaker object 514 may be created in a variety of ways. For example, the packet may be created by merely concatenating a web server identifier, speaker object identifier, or other identifier, to the session key and URL request received from the user. Alternatively, speaker object 514 may sign the packet by encrypting it with the private key. The private key could be pre-programmed at speaker object 514, or may be received from trusted network 138 (not shown). The packet is created in such a way when listener object 230 receives the packet, the packet can be identified as originating from speaker object 514."

As is clear from the above noted passage, at no point is there any teaching or suggestion in Alegre that the content obtained from the database 134 in response to the network request packet and sent from the access server 222 to the web host 210 is encrypted and sent along with a decryption key as in the present invention as recited in the claims. Alegre simply teaches as per the above that the network request packet sent from the speaker object 514 of the web host 210 to the listener object 1212 of the access server 222 can be encrypted.

Alegre further teaches, for example, in col. 7, lines 38-43 that:

> "When speaker object 514 receives a response to the request from access server 222 (step 1116), speaker object 514 creates a web page based on the response and sends the web page to session manager 510 for transmission to client browser (step 1118)."

Further, as is clear from the above noted passage, at no point is there any teaching or suggestion in Alegre that the web page generated by the speaker object 514 of the web host 210 based on the content obtained from the database 134 and sent from the web host 210 to the client 110 is encrypted and sent along with a decryption key as in the present invention as recited in the claims. No mechanism for the encryption and decryption of the content and web page returned in response to the network request packet is taught by Alegre.

As per the above there is no teaching or suggestion in Alegre that the content from the database 134 sent by the access server 222, nor the web page generated based on the content and sent by the web host 210 are encrypted and sent along with a decryption key as in the present invention. Alegre simply teaches that the network request packet sent from the speaker object 514 of the web host 210 to the listener object 1212 of the access server 222 can be encrypted.

Thus, both Datta and Alegre fail to teach or suggest that the requested contents from the contents expected to be in demand in the future are distributed to a client only when the distribution of the content to the client is permitted as recited in the claims.

Further, both Datta and Alegre fail to teach or suggest that the requested contents distributed to the client having permission is encrypted and the encrypted requested contents is distributed along with a decryption key so that the client having permission can decrypt the encrypted requested contents using the decryption key upon reception thereof as recited in the claims.

Therefore, both Datta and Alegre fail to teach or suggest the features of the present invention as now more clearly recited in the claims. Accordingly, reconsideration and withdrawal of the 35 USC §102(e) rejection of claims 5-7, 10, 11 and 15 as being anticipated by Datta and reconsideration and withdrawal of the 35 USC §103(a) rejection of claims 8 and 9 as being unpatentable over Datta in view of Alegre are respectfully requested.

The above described deficiencies of Datta and Alegre are also evident in each of the other references of record, namely Scott, Horvitz and Li. Therefore, combining the teachings of Datta with one or more of Alegre, Scott, Horvitz or Li as suggested by the Examiner in the Office Action still fails to teach or suggest the features of the present invention as now more clearly recited in the claims.

Scott is merely relied upon by the Examiner for an alleged teaching that the contents from the server can be received in a time zone when there is sufficient network bandwidth. Horvitz is merely relied upon by the Examiner for an alleged of the estimating of the likelihood that the user will transition to a particular URL. Li is merely relied upon by the Examiner for an alleged teaching of calculating a hit count tag that gives an indication of how many times a particular portion has been accessed and an importance tag that

gives a weight to the hit count and determines how the portion can stay in cache.

However, as is clear from the above, none of the other references utilized by the Examiner to reject the claims, namely Scott, Horvitz and Li, teach or suggest the above described features now more clearly recited in the claims wherein the requested contents from the contents expected to be in demand in the future are distributed to a client only when distribution of the content to the client is permitted and wherein the requested contents distributed to the client having permission is encrypted and the encrypted requested contents is distributed along with a distribution key so that the client having permission can decrypt the encrypted requested contents using the decryption key upon receipt thereof as in the present invention as now more clearly recited in the claims.

Therefore, Datta whether taken individually or in combination with one or more of Alegre, Scott, Horvitz and Li fail to teach or suggest the features of the present invention as now more clearly recited in the claims. Accordingly, reconsideration and withdrawal of the 35 USC §103(a) rejection of claims 13 and 17 as being unpatentable over Datta in view Scott, reconsideration and withdrawal of the 35 USC §103(a) rejection of claims 19, 21 and 23 as being unpatentable over Datta in view of Alegre and Horvitz and reconsideration and withdrawal of the 35 USC §103(a) rejection of claims 20, 22 and 24 as being unpatentable over Datta in view of Alegre and Li are respectfully requested.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with

respect to the references utilized in the rejection of claims 5-11, 13, 15, 17 and 19-24.

In view of the foregoing amendments and remarks, applicants submit that claims 5-11, 13, 15, 17 and 19-24 are in condition for allowance. Accordingly, early allowance of claims 5-11, 13, 15, 17 and 19-24 is respectfully requested.

To the extent necessary, Applicant petitions for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (520.40551X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120